Post-Quantum Secure Remote Password Protocol from RLWE Problem

Xinwei Gao[1], Jintai Ding[2]✉, Jiqiang Liu[1]✉, and Lin Li[1]

[1] Beijing Key Laboratory of Security and Privacy in Intelligent Transportation,
Beijing Jiaotong University, Beijing, 100044, P.R.China
{xinweigao, jqliu, lilin}@bjtu.edu.cn

[2] Department of Mathematical Sciences, University of Cincinnati, Cincinnati, 45219,
United States
jintai.ding@gmail.com

Abstract. Secure Remote Password (SRP) protocol is an augmented Password-based Authenticated Key Exchange (PAKE) protocol based on discrete logarithm problem (DLP) with various attractive security features. Compared with basic PAKE protocols, SRP does not require server to store user's password and user does not send password to server to authenticate. These features are desirable for secure client-server applications. SRP has gained extensive real-world deployment, including Apple iCloud, 1Password etc. However, with the advent of quantum computer and Shor's algorithm, classic DLP-based public key cryptography algorithms are no longer secure, including SRP. Motivated by importance of SRP and threat from quantum attacks, we propose a RLWE-based SRP protocol (RLWE-SRP) which inherit advantages from SRP and elegant design from RLWE key exchange. We also present parameter choice and efficient portable C++ implementation of RLWE-SRP. Implementation of our 209-bit secure RLWE-SRP is more than 3x faster than 112-bit secure original SRP protocol, 5.5x faster than 80-bit secure J-PAKE and 14x faster than two 184-bit secure RLWE-based PAKE protocols with more desired properties.

Keywords: Post-quantum, RLWE, SRP, PAKE, Protocol, Implementation

1 Introduction

1.1 Key Exchange

Key exchange (KE) is an important and fundamental cryptographic primitive. It allows two or multiple parties to agree on same session key, which is later utilized in encryption and other cryptographic primitives. With the ground-breaking Diffie-Hellman key exchange proposed in 1976 [14], public key cryptography came into reality and it has been widely deployed in real world applications. Since public key computations are rather expensive compared with symmetric-based ones, symmetric encryption is adopted to encrypt actual communication